National Institutes of Health
Office of the Chief Information Officer

www.ocio.nih.gov

AT A GLANCE:
Keeping NIH Secure

OVERVIEW

Protecting NIH's information and systems is one of the most important technology challenges facing the organization today. The Center for Information Technology (CIT) and the Office of the Chief Information Officer (OCIO), within the Office of the Director (OD), although separate in their structure and focus, work together under the same leadership to keep NIH secure and able to operate. The OCIO oversees NIH IT governance, policies, assessments, and information security, while CIT provides the infrastructure, operations, and services needed to achieve a secure IT environment.

INFORMATION SECURITY CHALLENGES FOR NIH

NIH has a large, complex IT environment that consists of approximately 45,000 staff distributed among more than 400 buildings and facilities in the Washington, DC and Maryland metropolitan areas, Arizona, Montana, and North Carolina. NIH's distributed IT environment makes achieving and maintaining security a challenge.

IT is an essential component of NIH's biomedical research activities, which increases the potential for a mission-impacting security compromise. Every day, NIH moves more than 71 terabytes of data to and from the Internet, more than 170 terabytes of data through the Internet2 (an advanced technology community and network founded by the nation's leading higher education institutions), and more than 5 petabytes of data within the NIH network.

Approximately 50,000 desktops and laptops, 15,000 servers, 11,000 mobile devices, 2,600 public-facing applications and websites, and a significant number of specialized computing devices routinely connect to the NIH network. Every day, CIT and OCIO deal with the realities of keeping NIH secure against significant and often sophisticated attacks aimed at NIH data, devices, and the network.

NIH has multiple layers of defensive mechanisms in place to provide prevention, detection, and containment capabilities. As of June 2019, NIH blocks 29 million emails (97% of the daily messages to NIH) and 7 million web connections due to spam or malicious content on a daily basis. In addition, NIH remediates 300,000 vulnerabilities against NIH systems and the network each month. Institutes and centers (ICs) submit 1,300 security-related service requests to the NIH Information Security Program monthly.

NIH Information Security Program

Protects over
110,000
devices
at NIH

Blocks over
29 million
malicious
emails daily

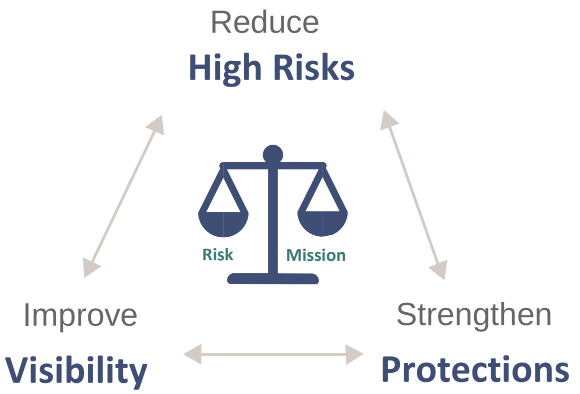
Serves over
45,000
NIH staff

Remediates
300,000
vulnerabilities
monthly

.

OCIO'S ROLE IN NIH INFORMATION

The NIH Information Security Program, an office within OCIO, works with CIT and other NIH ICs to implement security controls in their local environments consistent with NIH policy and standards.



Reduce **High Risks**

Improve **Visibility**

Strengthen **Protections**

The NIH Information Security Program takes a risk-based approach to information security. There are ongoing efforts to balance the risk to NIH networks, computers, data, and systems, while supporting NIH's biomedical research mission.

The NIH Information Security Program focuses on three key areas: **reduce high risks** in the NIH Information Technology environment; **improve visibility** of all devices supporting NIH or processing NIH data; and **strengthen protections** of all devices connecting to the NIH network. These security areas rely on a foundation of IT management best practices, including configuration management, patch management, system administration, penetration testing, change management, and training and awareness.

STAFF AWARENESS

Training and awareness are key components to securing NIH information and information systems against staff who may unknowingly cause harm to the networks by visiting websites infected with malware, responding to phishing emails, or storing or providing sensitive information in unsecured locations. The NIH Information Security Program ensures that NIH staff are properly trained on detection, prevention, and reporting procedures for malicious activity.

HOW CAN YOU HELP

Ensuring a secure environment for NIH requires commitment, effective communication, and collaboration. With that in mind, all NIH staff can play a role in preventing cyberattacks:

1. Work with your information systems security officer (ISSO) on potential security concerns.
2. Increase your security knowledge by visiting the NIH Information Security Awareness Gallery (https://ocio.nih.gov/InfoSecurity/AwarenessGallery/Pages/default.aspx), or the HHS Cybercare Library for information on topics such as encryption, identity theft, and more.
3. Report any lost or stolen equipment, security incidents such as compromised systems, attacks made on or to NIH computers, illegal or inappropriate use, abuse of computer privileges, or if you think you've been the victim of a phishing scam, to the NIH Information Security Program at NIHInfoSec@nih.gov or the NIH IT Service Desk (https://itservicedesk.nih.gov/).

GOING FORWARD

To protect NIH's most critical data and resources and ensure gaps in visibility and security controls are addressed, NIH must continue to invest in strengthening essential security infrastructure and information security and privacy capabilities. This effort will remove the blind spots for identifying risks, protect computers and devices on the NIH network, improve situational awareness and assessment of risks, and protect critical and sensitive data.

FOR MORE INFORMATION

To learn more about how OCIO keeps NIH secure, visit https://ocio.nih.gov.